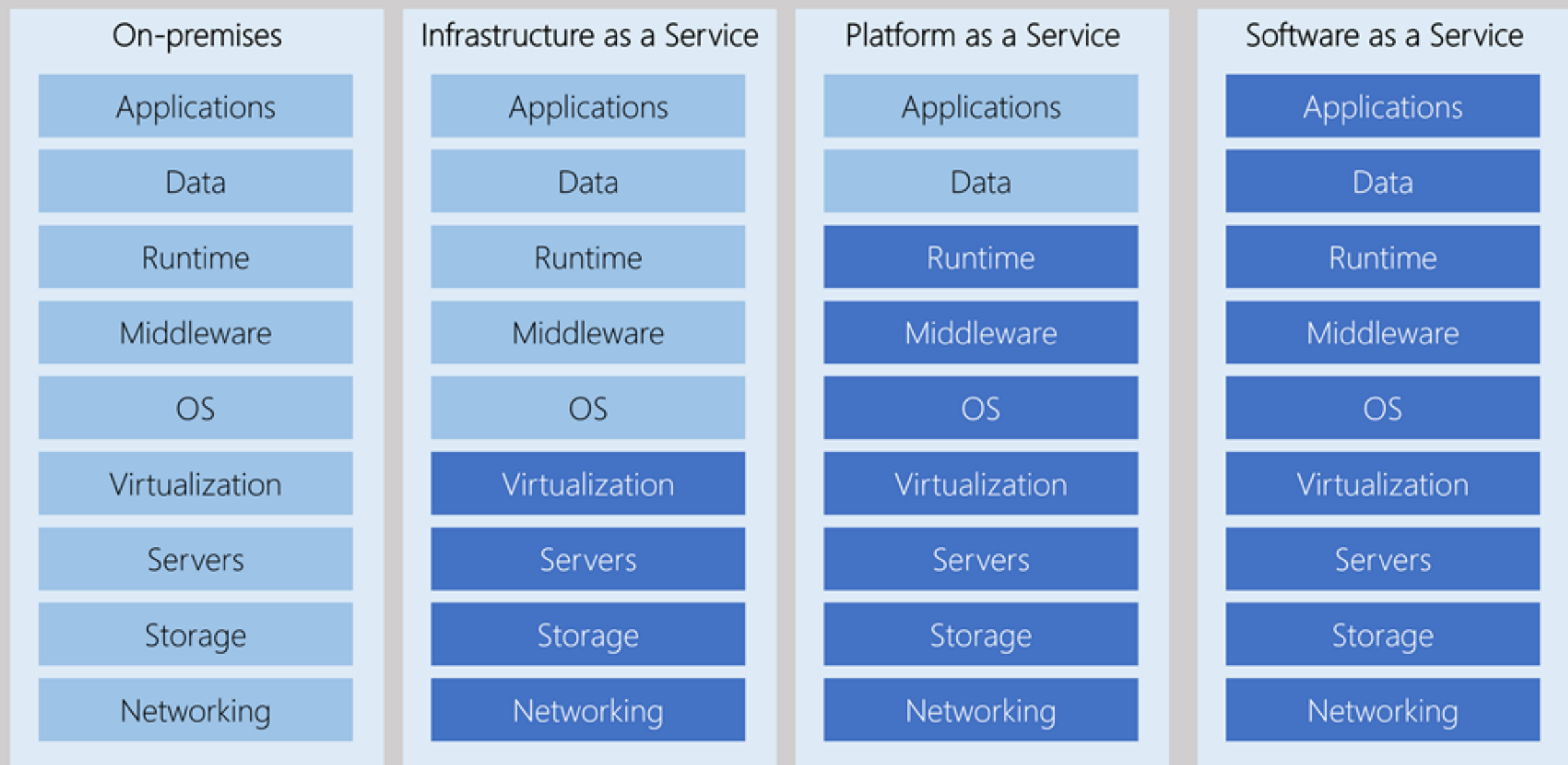


AZ 900 Azure Fundamentals学习笔记











You Manage



Provider Manages

Security & Management

-  Security Center
-  Azure portal
-  Azure Active Directory
-  Azure AD B2C
-  Multi-Factor Authentication
-  Automation
-  Key Vault
-  Azure Marketplace
-  VM Image Gallery
-  REST API and CLI

Media & CDN

-  Media Services
-  Media Analytics
-  Content Delivery Network








Integration

-  API Management
-  Service Bus
-  Azure Logic Apps







Compute Services

-  Container Service
-  VM Scale Sets
-  Azure Batch
-  Dev/Test Lab

Application Platform








-  Web Apps
-  Mobile Apps
-  API Apps
-  Cloud Services
-  Service Fabric
-  Notification Hubs
-  Functions

Developer Services

-  Visual Studio
-  Mobile Engagement
-  Azure DevOps
-  Xamarin
-  Application Insights
-  Visual Studio App Center

Platform Services







Data

-  SQL Database
-  SQL Data Warehouse
-  Cosmos DB
-  SQL Server Stretch Database
-  Azure Cache for Redis
-  Table Storage
-  Azure Search









Intelligence

-  Cognitive Services
-  Bot Services
-  Azure ML Studio

Analytics & IoT

-  HDInsight
-  Machine Learning
-  Stream Analytics
-  Data Catalog
-  Data Lake Analytics Service
-  Data Lake Storage
-  IoT Hub
-  Event Hubs
-  Data Factory
-  Power BI Embedded

Hybrid Cloud

-  Azure AD Connect Health
-  AD Privileged Identity Management
-  Domain Services
-  Backup
-  Azure Monitor
-  Import/Export
-  Azure Site Recovery
-  StorSimple

Infrastructure Services

Compute

-  Virtual Machines
-  Containers and Azure Kubernetes

Storage

-  Blob
-  Queues
-  Files
-  Disks

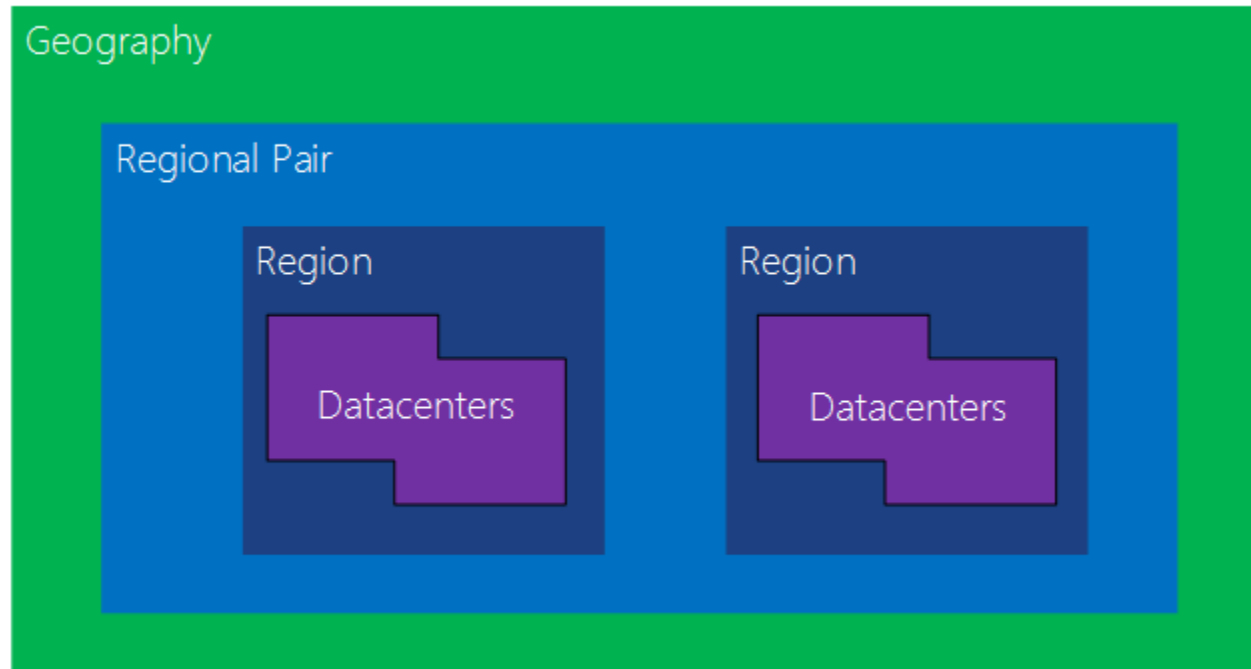
Networking

-  Virtual Network
-  Load Balancer
-  DNS
-  Express Route
-  Traffic Manager
-  VPN Gateway
-  App Gateway

Datacenter Infrastructure



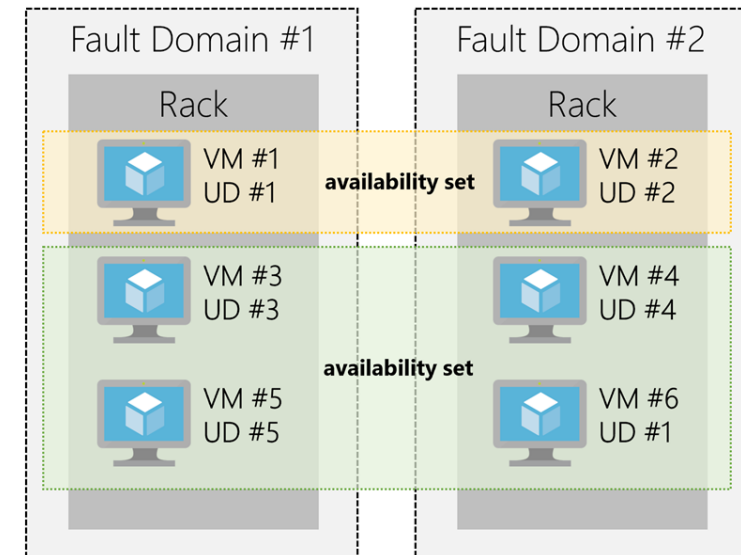
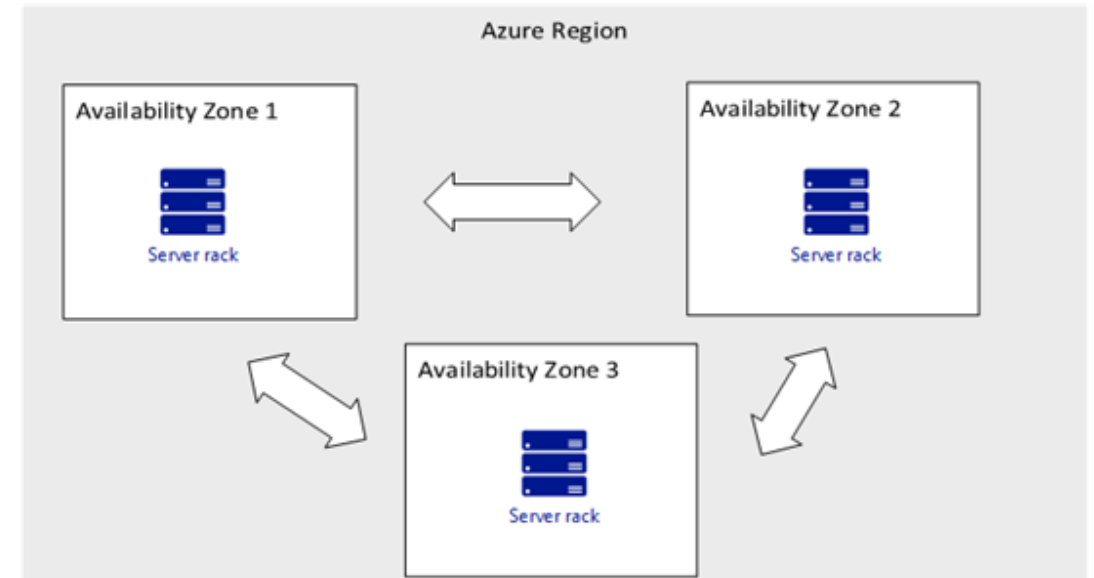
<https://azure.microsoft.com/en-us/global-infrastructure/geographies/>

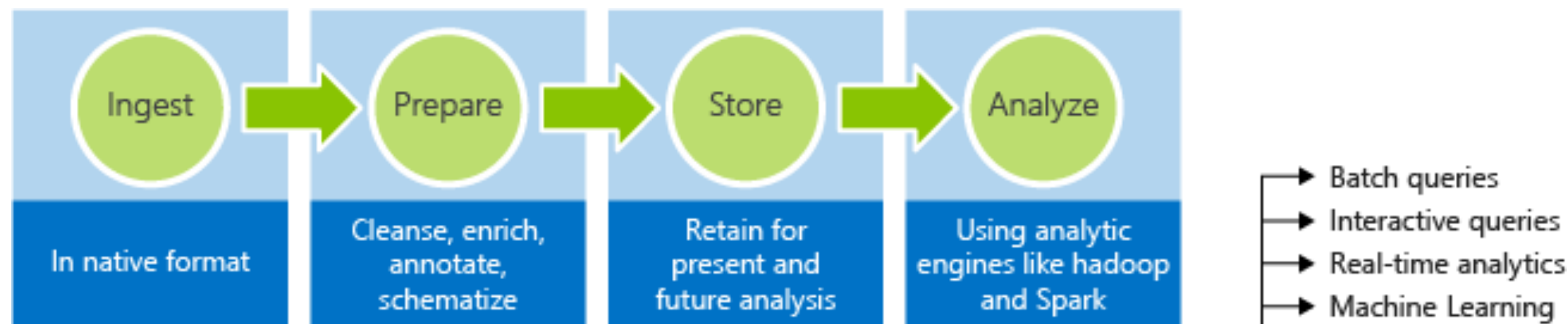


<https://social.technet.microsoft.com/wiki/contents/articles/51828.azure-vms-availability-sets-and-availability-zones.aspx>

This is the next level of Azure Virtual Machines high-availability, because Virtual Machines are in **different physical locations** within an Azure Region. It can be deployed using one or more Virtual Machines in an Azure Region. Availability zones offer 99.99% SLA.

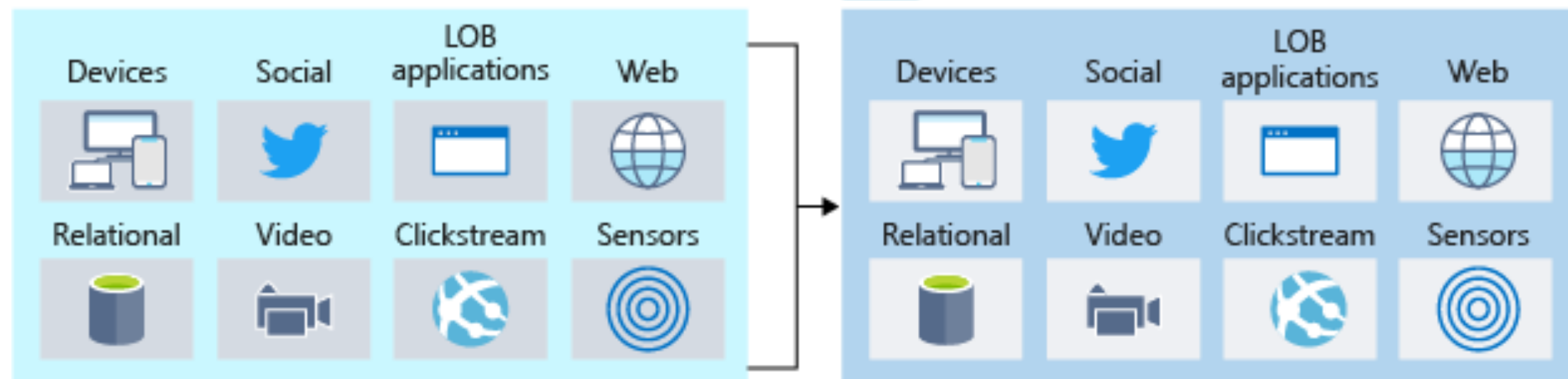
A group with two or more virtual machines in **the same Data Center** is called Availability Set, this ensures that at least one of the virtual machines hosted on Azure will be available if something happens. This configuration offers 99.95% SLA.













- Batch queries
- Interactive queries
- Real-time analytics
- Machine Learning
- Data Warehouse

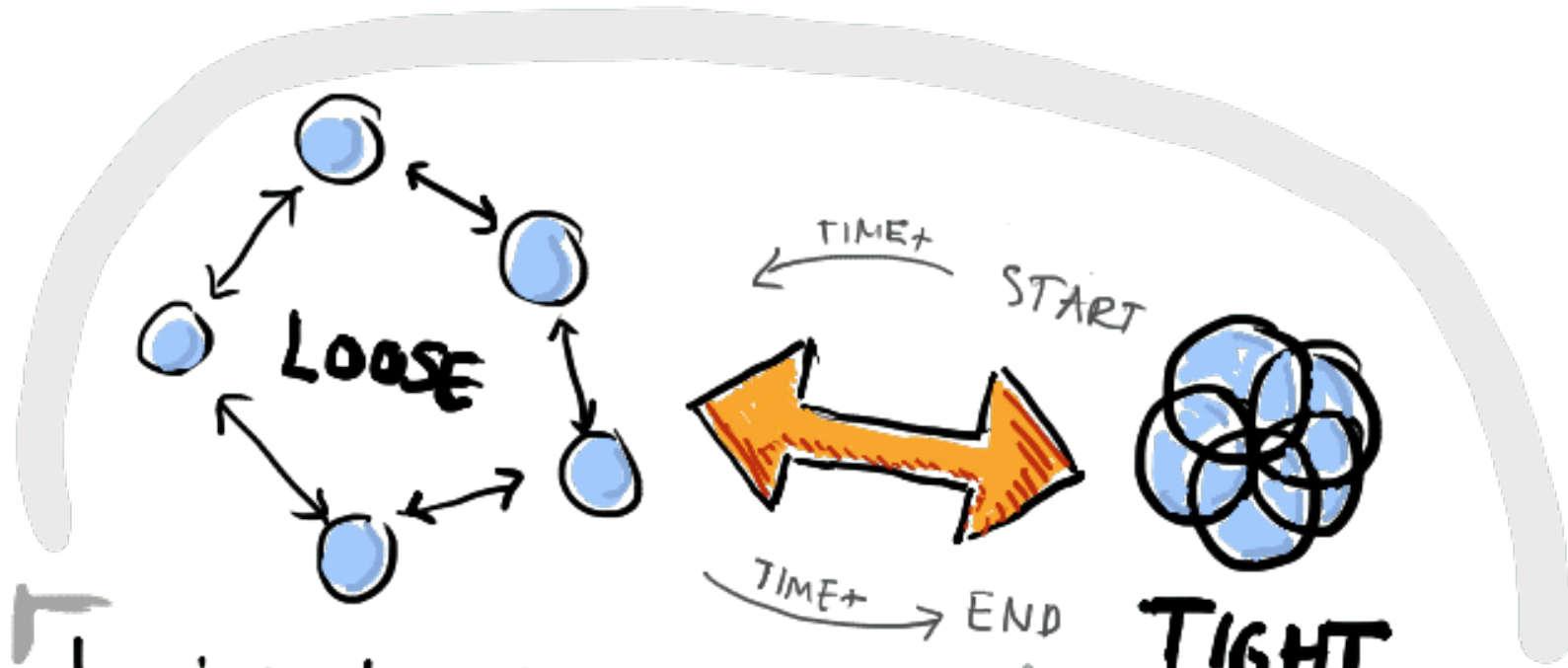
 Azure Data Lake Store



Needs		On-premises	Azure Data Storage
 Compliance and Security	1	Dedicated servers required for privacy and security	Client side encryption and encryption at rest
 Store structured and unstructured data	2	Additional IT resources with dedicated servers required	Azure Data Lake and portal analyzes and manages all types of data
 Replication and High Availability	3	More resources, licensing, and servers required	Built-in replication and redundancy features available
 Application sharing and access to shared resources	4	File sharing requires additional administration resources	File sharing options available without additional license
 Relational Data storage	5	Needs a database server with database admin role	Offers Database-as-a-Service option
 Distributed storage and data access	6	Expensive storage, networking, and compute resources needed	Azure Cosmos DB provides price-winning distributed access
 Messaging and load balancing	7	Hardware redundancy impacts budget and resources	Azure Queue provides effective load balancing
 Tiered storage	8	Management of tiered storage needs technology and labor skillset	Azure offers automated tiered storage of data

Benefits of using Azure to store data

- Here are some of the important benefits of Azure data storage:
- **Automated backup and recovery:** mitigates the risk of losing your data if there is any unforeseen failure or interruption.
- **Replication across the globe:** copies your data to protect it against any planned or unplanned events, such as scheduled maintenance or hardware failures. You can choose to replicate your data at multiple locations across the globe.
- **Support for data analytics:** supports performing analytics on your data consumption.
- **Encryption capabilities:** data is encrypted to make it highly secure; you also have tight control over who can access the data.
- **Multiple data types:** Azure can store almost any type of data you need. It can handle video files, text files, and even large binary files like virtual hard disks. It also has many options for your relational and NoSQL data.
- **Data storage in virtual disks:** Azure also has the capability of storing up to 8 TB of data in its virtual disks. This capability is significant when you're storing heavy data such as videos and simulations.
- **Storage tiers:** storage tiers to prioritize access to data based on frequently used versus rarely used information.



less interdependancy
less co-ordination
less information flow

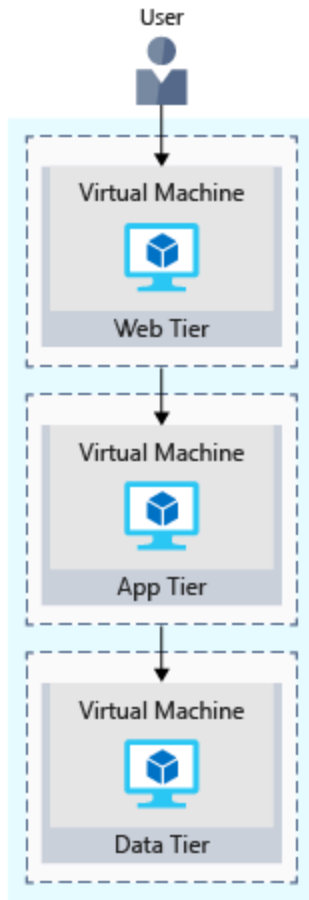
more interdependancy
more co-ordination
more information flow

LOOSE →

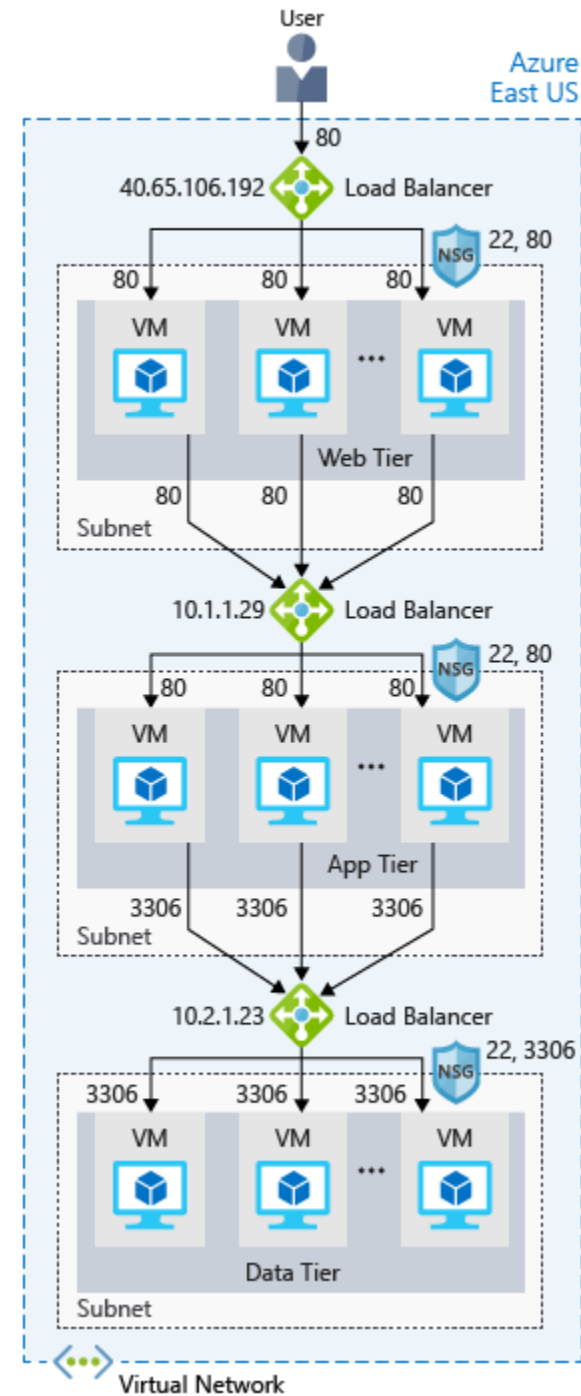
← TIGHT

DATA - STAMP - CONTROL - COMMON - CONTENT

N-tier architecture style

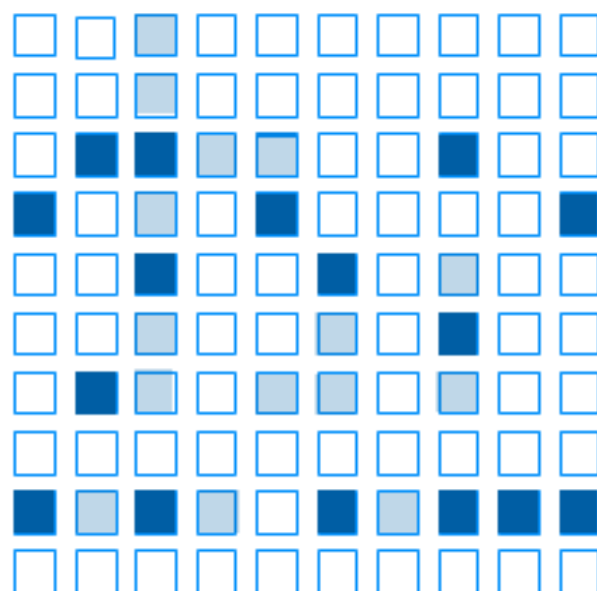


<https://docs.microsoft.com/en-us/azure/architecture/guide/architecture-styles/n-tier>

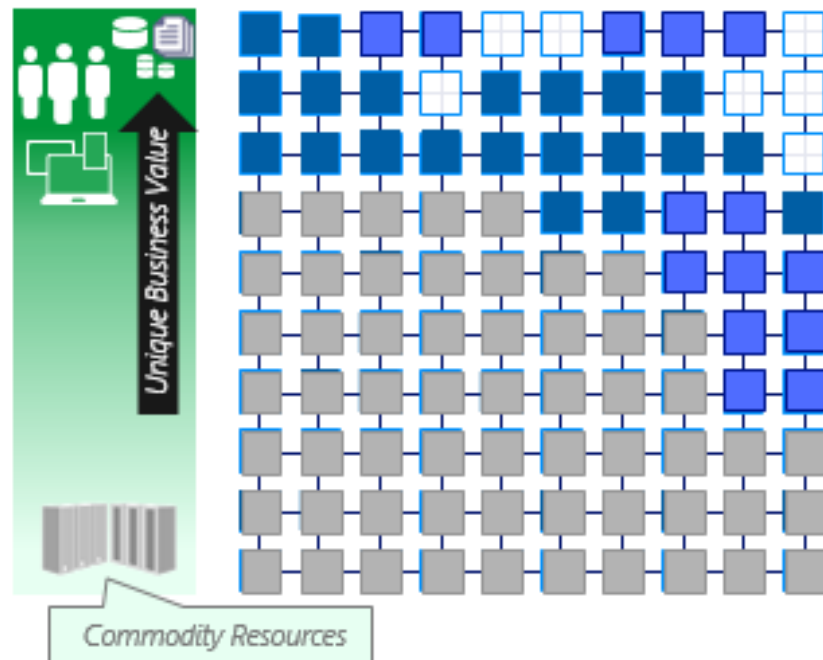


Security Advantages of Cloud Era

TRADITIONAL APPROACH



CLOUD-ENABLED SECURITY



Cloud Technology enables security to:

- Shift commodity responsibilities to provider and re-allocate your resources
- Leverage cloud-based security capabilities for more effectiveness
- ⊠ Use Cloud intelligence improve detection/response/time

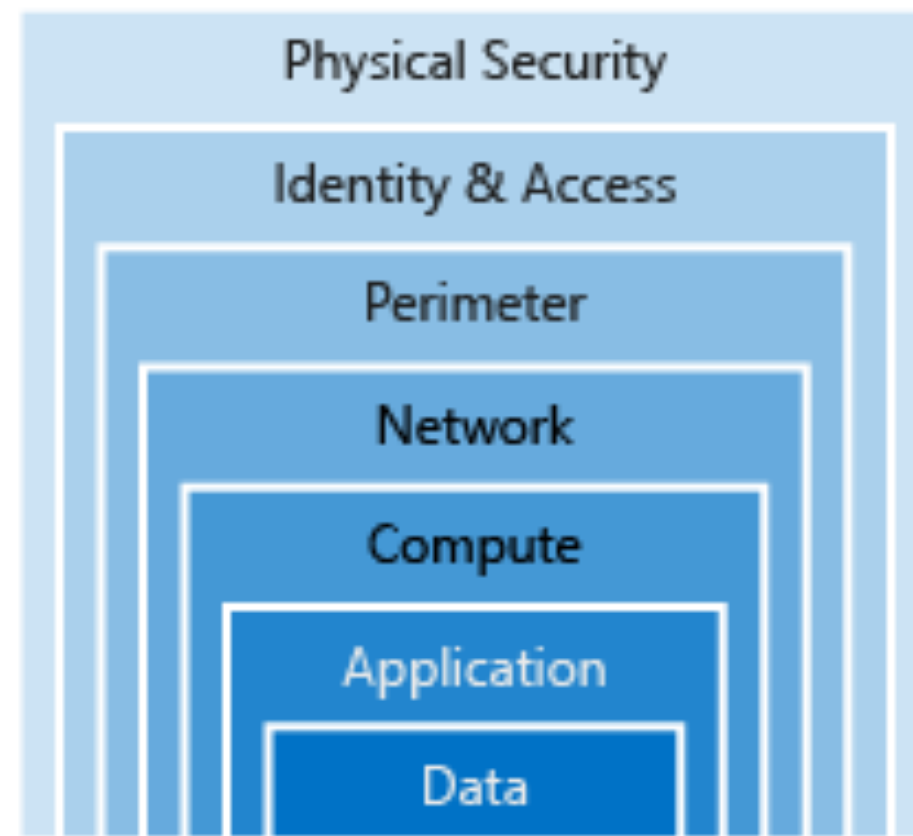
Security is a challenging and under-resourced function

- | | |
|--------------------------------|--|
| ■ Satisfied responsibility | □ Unmet responsibility |
| ■ Partially met responsibility | ■ Cloud Provider responsibility (Trust but verify) |

Security Layers

Responsibility	On-prem	IaaS	PaaS	SaaS
Data governance & rights management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account & access management	Customer	Customer	Customer	Customer
Identity & directory infrastructure	Customer	Customer	Microsoft	Microsoft
Application	Customer	Customer	Microsoft	Microsoft
Network controls	Customer	Customer	Microsoft	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft	Microsoft

■ Microsoft ■ Customer






[Perimeter networks](#) enable secure connectivity between your cloud networks and your on-premises or physical datacenter networks, along with any connectivity to and from the internet. They're also known as demilitarized zones (DMZs).

- Perimeter networks make use of the following Azure features and services:
- [Virtual networks](#), [user-defined routes](#), and [network security groups](#)
- [Network virtual appliances](#) (NVAs)
- [Azure Load Balancer](#)
- [Azure Application Gateway](#) and [web application firewall](#) (WAF)
- [Public IPs](#)
- [Azure Front Door](#) with [web application firewall](#)
- [Azure Firewall](#)

Cont.

- Perimeter networks are useful because you can focus your network access control management, monitoring, logging, and reporting on the devices at the edge of your Azure virtual network. A perimeter network is where you typically enable distributed denial of service (DDoS) prevention, intrusion detection/intrusion prevention systems (IDS/IPS), firewall rules and policies, web filtering, network antimalware, and more. The network security devices sit between the internet and your Azure virtual network and have an interface on both networks.
- Based on the Zero Trust concept mentioned earlier, we recommend that you consider using a perimeter network for all high security deployments to enhance the level of network security and access control for your Azure resources. You can use Azure or a third-party solution to provide an additional layer of security between your assets and the internet:
- Azure native controls. [Azure Firewall](#) and the [web application firewall in Application Gateway](#) offer basic security with a fully stateful firewall as a service, built-in high availability, unrestricted cloud scalability, FQDN filtering, support for OWASP core rule sets, and simple setup and configuration.
- Third-party offerings. Search the [Azure Marketplace](#) for next-generation firewall (NGFW) and other third-party offerings that provide familiar security tools and significantly enhanced levels of network security. Configuration might be more complex, but a third-party offering might allow you to use existing capabilities and skillsets.

RBAC

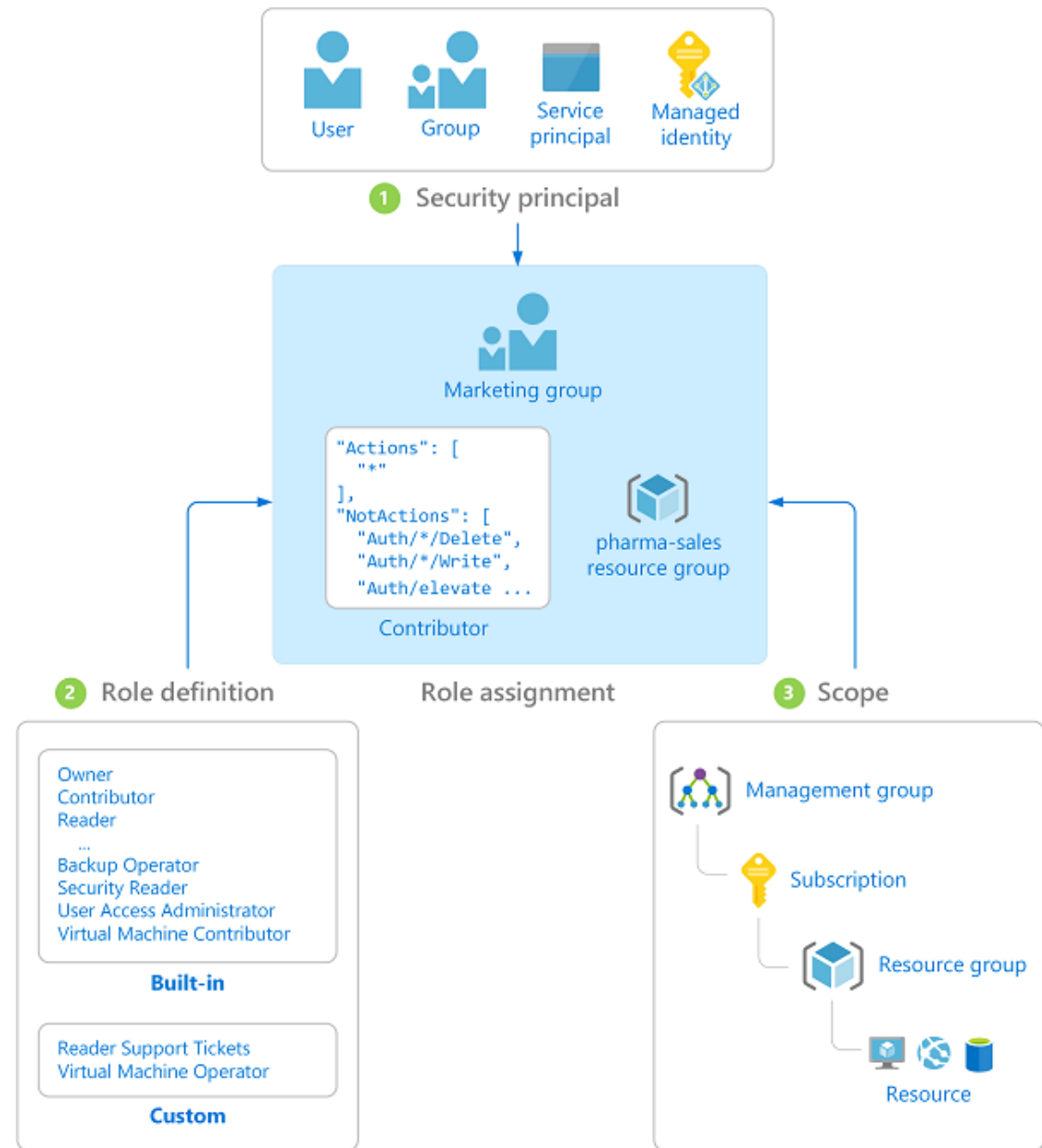
		Role			
		Reader	Resource-specific or custom role	Contributor	Owner
Scope	 Subscription	Observers	Users managing resources		Admins
	 Resource group				
	 Resource	Automated processes			

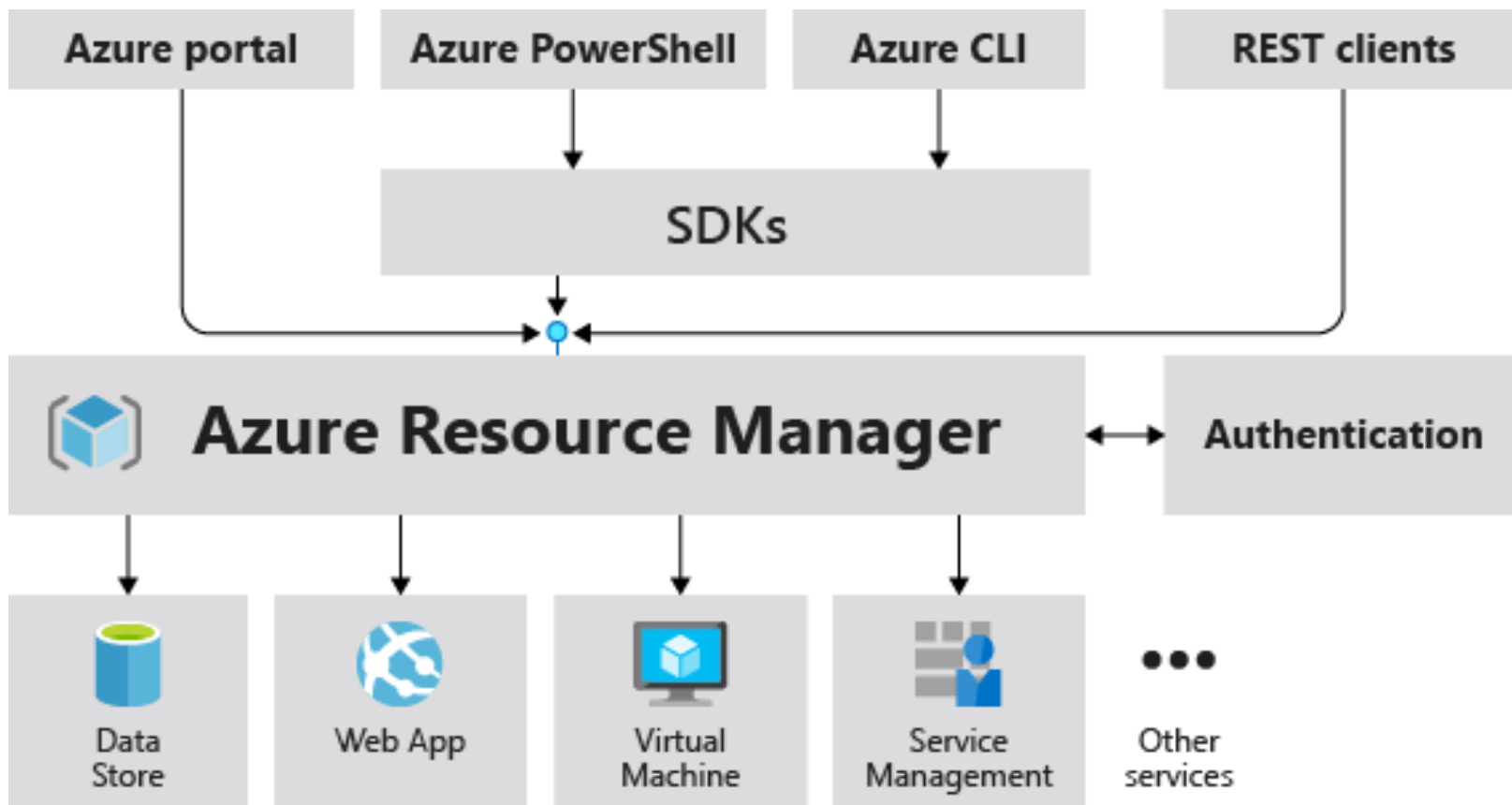
- How are Azure Policy and RBAC different?
- At first glance, it might seem like Azure Policy is a way to restrict access to specific resource types similar to role-based access control (RBAC). However, they solve different problems. RBAC focuses on *user actions at different scopes*. You might be added to the contributor role for a resource group, allowing you to make changes to anything in that resource group. Azure Policy focuses on *resource properties during deployment* and for already-existing resources. Azure Policy controls properties such as the types or locations of resources. Unlike RBAC, **Azure Policy is a default-allow-and-explicit-deny system.**

<https://docs.microsoft.com/en-us/azure/role-based-access-control/overview>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

RBAC





	BASIC	DEVELOPER	STANDARD	PROFESSIONAL DIRECT	PREMIER
		Purchase support	Purchase support	Purchase support	Contact Premier
Scope	Available to all Microsoft Azure accounts	Microsoft Azure: Trial and non-production environments	Microsoft Azure: Production workload environments	Microsoft Azure: Business-critical dependence	All Microsoft Products, including Azure: Substantial dependence across multiple products
Customer Service, Self-Help and Communities	24x7 access to billing and subscription support, online self-help, documentation, whitepapers, and support forums	24x7 access to billing and subscription support, online self-help, documentation, whitepapers, and support forums	24x7 access to billing and subscription support, online self-help, documentation, whitepapers, and support forums	24x7 access to billing and subscription support, online self-help, documentation, whitepapers, and support forums	24x7 access to billing and subscription support, online self-help, documentation, whitepapers, and support forums
Best Practices	Access to full set of Azure Advisor recommendations	Access to full set of Azure Advisor recommendations	Access to full set of Azure Advisor recommendations	Access to full set of Azure Advisor recommendations	Access to full set of Azure Advisor recommendations
Health Status and Notifications	Access to personalized Service Health Dashboard & Health API	Access to personalized Service Health Dashboard & Health API	Access to personalized Service Health Dashboard & Health API	Access to personalized Service Health Dashboard & Health API	Access to personalized Service Health Dashboard & Health API
Technical Support		Business hours access ¹ to Support Engineers via email	24x7 access to Support Engineers via email and phone	24x7 access to Support Engineers via email and phone	24x7 access to Support Engineers via email and phone
Who Can Open Cases		Unlimited contacts / unlimited cases	Unlimited contacts / unlimited cases	Unlimited contacts / unlimited cases	Unlimited contacts / unlimited cases
Third-Party Software Support		Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting	Interoperability & configuration guidance and troubleshooting
Case Severity/Response Times		Minimal business impact (Sev C): <8 business hours ¹	Minimal business impact (Sev C): <8 business hours ¹ Moderate business impact (Sev B): <4 hours Critical business impact (Sev A): <1 hour	Minimal business impact (Sev C): <4 business hours ¹ Moderate business impact (Sev B): <2 hours Critical business impact (Sev A): <1 hour	Minimal business impact (Sev C): <4 business hours ¹ Moderate business impact (Sev B): <2 hours Critical business impact (Sev A): <1 hour <15 minutes (with Azure Rapid Response or Azure Event Management)
Architecture Support		General guidance	General guidance	Architectural guidance based on best practice delivered by ProDirect Delivery Manager	Customer specific architectural support such as design reviews, performance tuning, configuration and implementation assistance delivered by Microsoft Azure technical specialists.
Operations Support				Onboarding services, service reviews, Azure Advisor consultations	Technical account manager-led service reviews and reporting
Training				Azure Engineering-led web seminars	Azure Engineering-led web seminars, on-demand training
Proactive Guidance				ProDirect Delivery Manager	Designated Technical Account Manager
Launch Support					Azure Event Management (available for additional fee)
Pricing		\$29/mo	\$100/mo	\$1,000/mo	Contact us

Support Model

Azure App Service

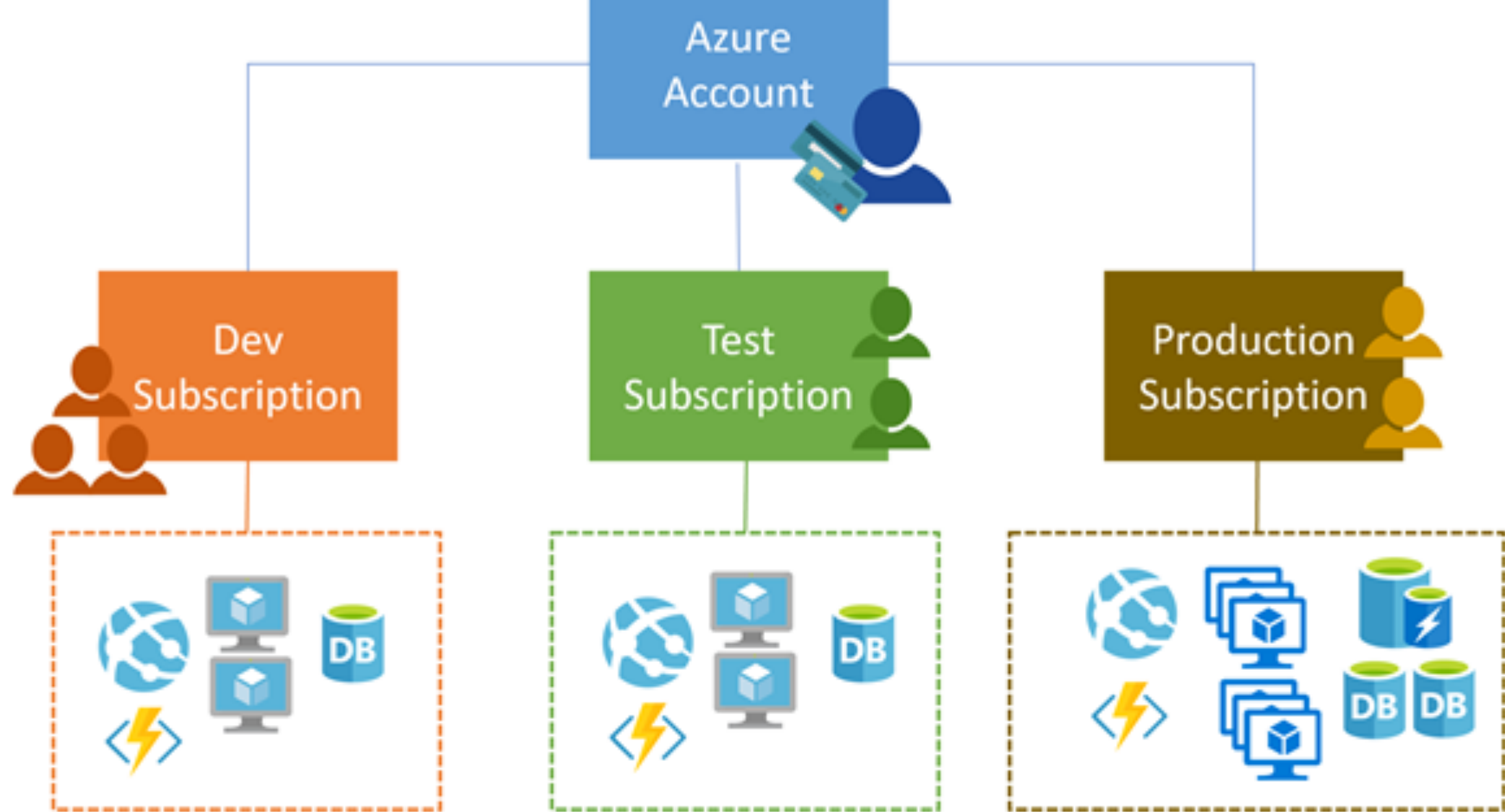


build and host web apps, mobile back ends, and RESTful APIs

offers auto-scaling and high availability

supports both Windows and Linux

enables automated deployments



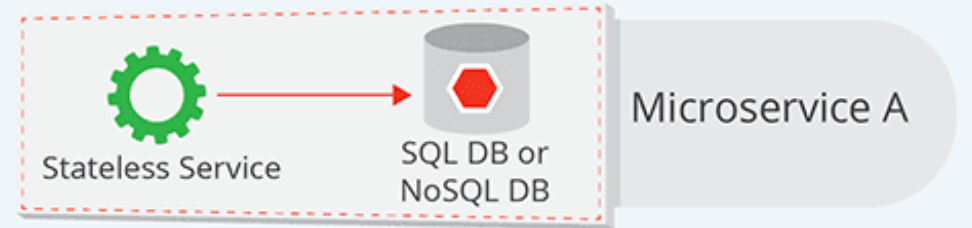
- **Stateful vs. Stateless – An Overview**

- The [key difference](#) between stateful and stateless applications is that stateless applications don't "store" data whereas stateful applications require backing storage. Stateful applications like the Cassandra, MongoDB and MySQL databases all require some type of persistent storage that will survive service restarts.

- Keeping state is critical to running a stateful application whereas any data that flows via a stateless service is typically transitory and the state is stored only in a separate back-end service like a database. Any associated storage is typically ephemeral. If the container restarts for instance, anything stored is lost. As organizations adopt containers, they tend to begin with stateless containers as they are more easily adapted to this new type of architecture and better separated from their monolithic application codebase, thus they are more amenable to independent scaling.

Stateful and Stateless Applications

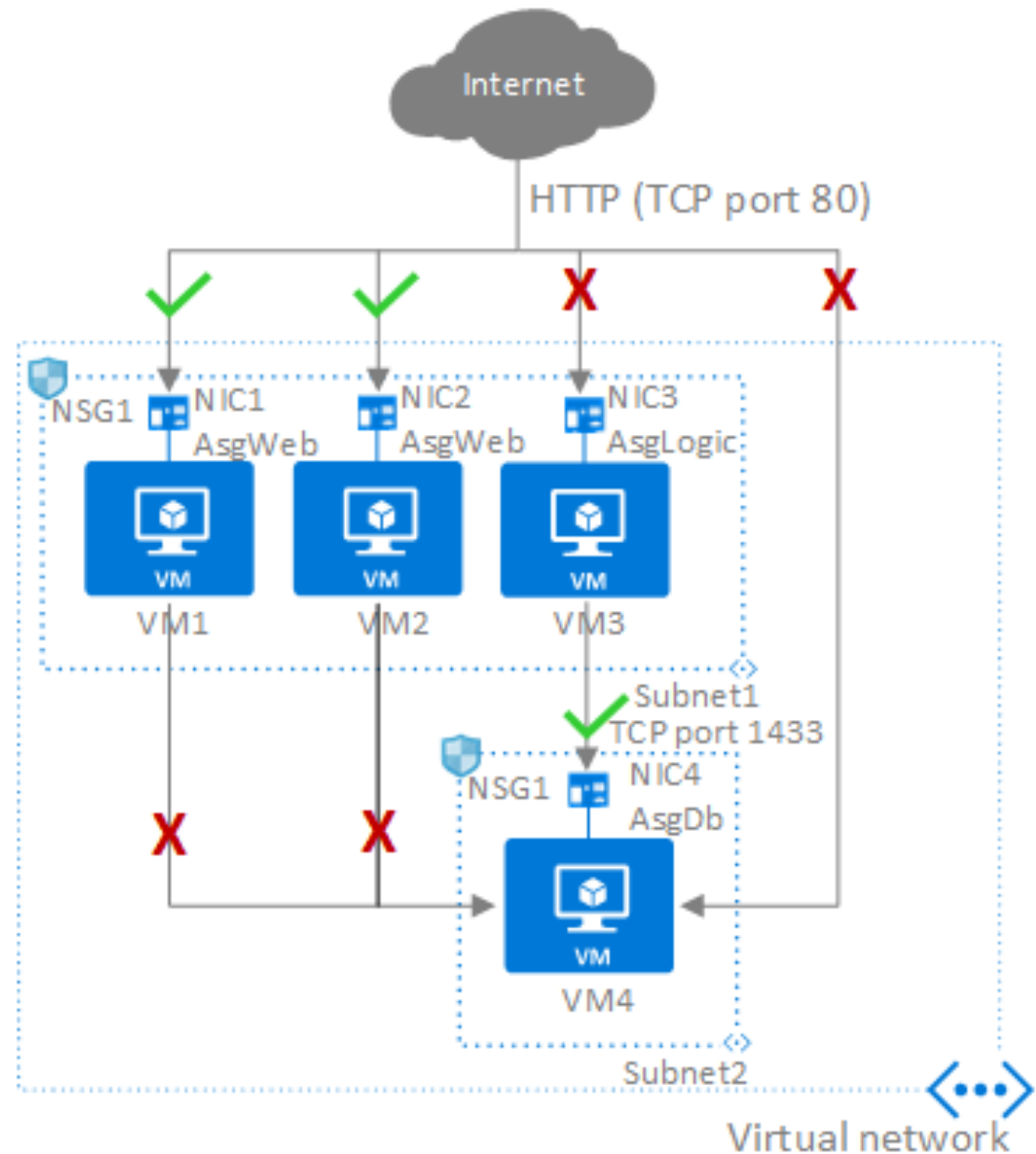
Stateless Services



Stateful Services



Understand NSG



Exam Notes

<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview>

- An Azure storage account contains all of your Azure Storage data objects: blobs, files, queues, tables, and disks. The storage account provides a unique namespace for your Azure Storage data that is accessible from anywhere in the world over HTTP or HTTPS. Data in your Azure storage account is durable and highly available, secure, and massively scalable.

- **Azure Firewall allows you to centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks**
- **2000 role assign of each subscription**
- Previously, RBAC was an allow-only model with no deny, but now RBAC supports deny assignments in a limited way. **Explicitly allow and deny.**

VS.

Policy is default allow and explicitly deny

- Multiple **subscriptions can trust** the same **Azure AD directory**, but each **subscription can only trust a single directory.**

- Cognitive API can do everything for a set of APIs on image, voice...
- Which of the following features is included in the Standard Support plan that is not available to the Developer Support plan? 24*7 access vs Business hour access
- 1000 VM per VM scale set. A group of identical, load-balanced VMs. 区分availability set
- Rest API/SDL can deploy as well
- What service does Azure provide as an optional upgrade to protect against DDoS attacks? Basic to Standard
- AZ is for high availability, Availability set for maintenance – 更新yu, 故障yu
- Reserved Instances often offer 40% or more savings off of the price of pay-as-you-go virtual machines
- VM is IAAS – need to manage OS!
- You cannot perform a task that violates policy, so you have to remove the policy in order to perform the task.
- **Log Analytics Workplace – create to collect logs and metrics, correlate events from multiple resources**
- Content Delivery Network - allows you to improve performance by removing the burden of serving static, unchanging files from the main server to a network of servers around the globe; a CDN can reduce traffic to a server by 50% or more, which means you can serve more users or serve the same users faster; SaaS

A content delivery network (CDN) is a distributed network of servers that can efficiently deliver web content to users. CDNs store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.

- Azure SQL Database is DaaS and PaaS
- Cosmos DB - extremely low latency (fast) storage designed for smaller pieces of data quickly; SaaS
- Application Gateway and Load Balancer can both Load balance, add-on is WAF. Also Application gateway can make load balancing decisions based on the URL path, while a load balancer can't.
- **But how many subscriptions can a single account be associated with? – no limit**
- **PowerShell vs CLI – just personal choice, no additional benefit**
- Functions are designed for short pieces of code that start and end quickly – not for batch, continuous run. Can use code editor in Azure Portal
- Azure Policy can add restrictions on storage account SKUs, virtual machine instance types, and rules relating to tagging of resources and groups. It cannot prompt a user to ask them if they are sure, or update security batch
- GA - anyone can use it what so ever. Private Preview = must apply to use

- Security Center – one of the Security Service. Detect and protect threats, get security solution and recommendation. Also can see compliance dashboard
- Compliance Manager – workflow based score, hosted on Trust Portal
- Privacy Statement
- MCS Trust Center – list of security , privacy , compliance, transparency standards (these are also ‘Azure Security’)
- Service Trust Portal – list of standards, reports, whitepapers, 3rd party
- Azure Monitor vs Service Health

One is metrics and logs of performance of App, identify issues and optimize

One is azure status (global), service health (personal) and resource health(deeper)

- **IaaS examples – VM, Virtual Network (physical datacenter, network, servers and storage)**
- **PaaS – Azure App Service, just need code + configuration. Azure SQL Server, VPN gateway**
- IaaS is easiest for migrating current hosted application. Lift and shift
- Elasticity saves you money during slow periods (over night, over the weekend, over the summer, etc) and also allows you to handle the highest peak of traffic.
- Each Azure free account includes 1 free Windows VM and 1 free Linux VM per month, for the first 12 months.
- Subnet purpose: For security purposes, you should not allow "port 80" web traffic to reach certain servers, and you do that by having separate NSG rules on each subnet.
- Privileged Identity Management can be used to ensure privileged users have to jump through additional verification because of their role.
- Computing Resources - Serverless Functions Apps and Logics App ARE computing resources! Azure App Service, Container
- **AD Connect** – sync corporate AD with Azure AD
- VM – ONLY windows and linux!
- Region special case before choose - Some regions of the world require special contracts with the local provider such as Germany and China.
- Firewall is not network layer!!! Perimeter layer
- Initiative - An *initiative definition* is a set or group of policy definitions to help track your compliance state for a larger goal
- Subscriptions can be nested and placed into management groups to make managing them easier.

- SLAs are not for preview or services free of charge/free accounts
- Azure Advisor – High availability, security, performance, cost
- <https://samcogan.com/azure-monitor-and-azure-log-analytics-when-to-use-which/>
- <https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/>